Quick Reference Guide

for Microsoft Windows XPe-based Thin Clients

t5000 Series

Document Part Number: 253378-006

January 2005

This guide supplements the standard Microsoft Windows XPe documents supplied by Microsoft Corporation. This document highlights the differences, enhancements, and additional features provided with this terminal.

WARNING: Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

Quick Reference Guide

for Microsoft Windows XPe-based Thin Clients
t5000 Series

SixthEdition (January 2005)

Document Part Number: 253378-006

Introduction

HP Compaq t57x0 thin client models use the Microsoft Windows XP Embedded (XPe) operating system. These thin clients provide access to applications, files, and network resources made available on machines hosting Citrix ICA and Microsoft RDP session services. Only the keyboard, mouse, audio/video, and display data are transmitted over the network between the thin clients and session servers.

Image Updates

HP provides periodic updates to the image for the HP Compaq t57x0 thin clients. Check the HP support site for important documentation that provides specific information for your image version. Support documentation can be found at

http://welcome.hp.com/country/us/en/support.html

This guide provides information about the Microsoft Windows XPe. Please see the "Microsoft Windows XPe Service Pack 2 (SP2)" section of this guide for more details about the new features provided by this image.

Server Environment Requirements

These thin clients use a variety of services accessed through the network. These include session and product support services as well as standard network services such as DHCP and DNS. The following session and support services are required:

Session Servers

Any of the following session services must be available on the network where your thin client is connected.

Citrix ICA

Citrix Independent Computing Architecture (ICA) can be made available on the network using either of the following services:

- Microsoft Windows 2000 Server with Terminal Services and one of the following installed:
  - Citrix MetaFrame 1.8 (alone or with Service Packs 2 or 3 FR1)
  - Citrix MetaFrame XP
- Microsoft Windows NT 4.0 Terminal Server Edition with Citrix MetaFrame 1.8 installed.

Microsoft RDP

Microsoft Remote Desktop Protocol (RDP) services are accessed by the Terminal Services Client application on the thin client. RDP can be made available on the network using any of the following services:

- Microsoft Windows 2000 Server with Terminal Services installed
- Microsoft Windows NT 4.0 Terminal Server Edition
- Microsoft Windows XP Professional
- Microsoft Windows Server 2003

If a Windows 2000 server is used for both of these session services (ICA and RDP), a Terminal Services Client Access Licenses (TSCAL) server must also reside somewhere on the network. Client Access licenses permit clients to use the terminal, file, print and other network services provided by Windows 2000 Server. The server grants temporary licenses (on an individual device basis) that are good for 90 days. Beyond that, you must purchase TSCALs and install them in the TSCAL server (you cannot make a connection without a temporary or permanent license).

For additional information about Microsoft Terminal Services, access the Microsoft Web site at

http://www.microsoft.com/windows2000/technologies/terminal/default.asp

Terminal Emulation Support

Depending on your thin-client model, a third-party terminal emulation software is installed on the thin client to support computing on legacy platforms. The terminal emulation software uses the Telnet protocol to communicate with the computing platform.

Support Servers

The following support server is available to use with your thin-client network.

Altiris Deployment Solution

The Altiris Deployment Solution™ provides an easy-to-use, integrated tool that allows remote management of the thin clients throughout their entire lifecycle, including initial deployment, ongoing management, and software deployment.

The Altiris Deployment Solution must be installed on a Windows NT 4.0 or Windows 2000 Server or a workstation capable of logging on as administrator to a domain that provides specified network services, and which can access a software repository for your thin client. The Altiris Deployment Solutions software accesses your thin client through the factory-installed Preboot Execution Environment (PXE) client utilities. PXE upgrade services are built into the Altiris Deployment Solution.

For additional information about the Altiris Deployment Solution, refer to the Altiris Web site at: www.altiris.com/documentation and review the *Altiris Deployment Solution User Guide*.

Extended Windows XPe Features

The operating system of the Microsoft Windows XPe-based thin client has extended features not found in the standard Microsoft Windows XP operating system. With the exception of the Microsoft Terminal Server Client (Remote Desktop Connection Manager) and Citrix Program Neighborhood, and possibly a special-order terminal emulation application, if installed, controls for extended Windows XPe features are only available through the Administrator logon account.

CAUTION: A write filter is employed on the thin client for security and to prevent excessive flash write activity. Changes to the thin client configuration are lost when the thin client is restarted unless the write filter cache is disabled or a **-commit** command is issued during the current boot session. See the write filter topics in "Microsoft Windows XPe Service Pack 2 (SP2)" on page 19 of this guide for instructions disabling the cache. Remember to always enable the write filter when you no longer want changes to be permanent.

Logging On

You can log on to your thin client using automatic log on or manual log on.

Automatic Logon

The default for the XPe-based thin client is automatic logon. The administrator can use the HP Logon Manager in the Control Panel to enable/disable auto logon and change the auto logon user name, password, and domain. Only the administrator logon account can change auto logon properties.

To save changes, be sure to disable the write filter cache or issue the **-commit** command anytime during the current boot session. See "Enhanced Write Filter Manager" on page 30 of this guide for information about the write filter and instructions for disabling write filter. Remember to enable the write filter when you no longer want changes to be permanent.

The Log On to Windows dialog box is bypassed if automatic logon is enabled. If you want to log on as a different user while auto logon is enabled, Press and hold down the **Shift** key while clicking **Start > Shut Down > Log Off...** This will cause the Log On to Windows dialog box to display and allow you to manually enter the logon information.

Manual Logon

When automatic logon is not enabled, upon thin client startup the Log On to Windows dialog box displays.

Type the logon information in the User Name and Password text boxes. Note the following:

- For a user logon account, the factory-default user name and password are both **User** (enter in both text boxes).
- For an administrator logon account, the factory-default user name and password are both **Administrator** (enter in both text boxes).

For security purposes, it is recommended that the passwords be changed from the defaults. An administrator can change passwords by pressing **Ctrl+Alt+Del** to open the Windows Security dialog box and then selecting Change Password. The password cannot be changed when logged on as a user.

Passwords are case sensitive but user names are not.

The administrator may create additional user accounts by using the User Accounts utility available through the Administrative Tools option in Control Panel. However, due to local memory constraints, the number of additional users should be kept to a minimum. See “User Log Accounts” on page 36 of this guide for instructions.

Administrator Logon Access

To access Administrator logon, regardless of the state of the thin client User Mode, do the following:

While holding down the "Shift" key, use the mouse to initiate logoff of the User (invoked from the Start menu).

The logon screen will then appear for Administrator logon.

The default username and password for the Administrator account is "Administrator". The default username and password for the User account is "User".

The HP Manager application can be used to permanently modify the default login user. It is located in the control panel, and can only be accessed and modified by the Administrator.

Pre-installed Utilities

There are several preinstalled utilities on the thin client. The following section discusses these utilities.

Altiris Client Agent

The Altiris Client Agent resides on the thin client. This agent allows the Altiris server to discover valid clients that are added to the network. The agent carries out assignments and reports the status of individual thin clients to the Altiris server.

Citrix Program Neighborhood

Citrix Program Neighborhood is a feature of ICA introduced with MetaFrame 1.8 that enables users to connect to MetaFrame and WinFrame servers and published applications. Program Neighborhood allows complete administrative control over application access and delivers an even greater level of seamless desktop integration.

Enhanced Write Filter Manager

Upon system boot, the Enhanced Write Filter Manager utility is automatically launched. The write filter provides security and protects the flash memory from excessive write activity. See "Enhanced Write Filter Manager" on page 30 of this guide for information about the write filter.

Changes made to the thin client configuration will be lost when the thin client is rebooted unless the write filter cache is disabled or a **-commit** command is issued during the current boot session. See "Enhanced Write Filter Manager" on page 30 of this guide for instructions on how to disable the write filter. Remember to enable the write filter when you no longer want changes to be permanent.

Macromedia Flash Player

Macromedia Flash Player is the agent for rich web experiences across multiple platforms. With Macromedia Flash Player, web users worldwide can view and interact with content developed in Macromedia Flash.

Remote Desktop Connection

The Microsoft Remote Desktop Connection allows an administrator to access a Windows XPe-based thin client from a remote location. With this connection the administrator can take control of the local thin client and its applications.

The XPe Desktop

This section gives a general overview of the XPe User and Administrator desktop features and functions.

User's Desktop

The desktop that displays when you are logged on as a user is a standard Windows XP desktop, except that the Citrix Program Neighborhood and Remote Desktop Connection and Internet Explorer are the only icons present. These selections are also available from the Start menu. If the terminal emulator application is installed, it may be opened from the **Start > Programs** menu.

Links to remote ICA NFuse-published applications may also be listed on the Start menu and/or displayed as icons on the desktop. Refer to the Citrix NFuse 1.6 documentation for information and instructions.

For information pertaining to the functionality of the standard Windows XPe desktop and Start menu items, refer to the applicable Microsoft documentation that can be found at

www.microsoft.com/windows/embedded/xp/default.asp

See "Programs Menu Extended Selections" on page 12 of this guide for the Internet locations of the Citrix Program Neighborhood and Remote Desktop Connection help documents.

The Control Panel, available to a user through **Start > Control Panel,** provides access to a limited set of resources for making Windows XPe user preference settings. You must be logged on as administrator to access the extended set of system resources.

Right-clicking the mouse when the pointer is on your desktop background does not open a popup menu.

You may copy and paste text between remote session and local computer by using standard copy and paste methods.

Administrator's Desktop

The desktop that appears when you are logged on as an administrator is a standard Windows XP desktop. Icons present on the default administrator desktop Start menu are My Computer, My Network Places, Citrix Program Neighborhood, Remote Desktop Connection, and Internet Explorer. The three application selections are also available from the Start menu. If the terminal emulator application is installed it may be opened from the **Start > Programs** menu. Extended resources available only to administrators may be accessed from the Start menu.

For information pertaining to the functionality of the standard Windows XPe desktop and Start menu items, refer to the Microsoft Web site as described in the previous section.

Right-clicking the mouse when the pointer is on the administrator's desktop background opens a popup menu.

Logging Off from, Restarting, and Shutting Down the Thin Client

To log off from, restart, or shut down the thin client, click **Start > Shut Down.** From the Shut Down dialog box select the desired action and click **OK.**

You may also log off or shut down using the Windows Security dialog box. Press **Ctrl+Alt+Del** to open the dialog.

If automatic logon is enabled, when you log off (without shutting down) the thin client immediately logs on the default user. See "Logging On" on page 5 of this guide for instructions for logging on as a different user.

The following utilities are affected by logging off, restarting, and shutting down the thin client:

Enhanced Write Filter

See "Enhanced Write Filter Manager" on page 30 of this guide for information about the Enhanced Write Filter. If you make changes to system configuration settings and want them to persist, you must disable the write filter cache or issue the **-commit** command during the current boot session. Otherwise, the new settings will be lost when the thin client is shut down or restarted. Always remember to enable the write filter when you no longer want changes to be permanent.

The write filter cache contents are not lost when you simply log off and on again (as the same or different user); that is, you may disable the write filter cache after the new logon and still retain the changes.

A user logon account does not have write filter disabling privileges; this is a local or remote administrator function.

Power Management

A "Monitor Saver" turns off the video signal to the monitor, allowing the monitor to enter a power-saving mode after a designated idle time. Parameters for this mode are available by right-clicking on the desktop background and selecting **Properties > Screen Saver > Power.**

System Time

After power-off, clock time will not be lost as long as the power source remains plugged in. Clock time will be lost, however, if the power source is unplugged. The local time utility may be set to synchronize the thin client clock to a time server automatically at a designated time or manually.

Correct time should be maintained because some applications may require access to the local thin client time. To open the Date and Time Properties dialog, click on the time area in the task bar or double-click the Date and Time icon in the Control Panel.

Programs Menu Extended Selections

Open the Programs menu by clicking **Start > Programs.** Additional selections available on the Programs menu are:

Citrix Program Neighborhood

This selection opens the Citrix Program Neighborhood window. This window, which also opens from a desktop icon, facilitates connections to remote applications running on ICA servers.

Documentation for the ICA client application is available from the Citrix Corporation Web site at:

www.citrix.com/support

(Search under Product Documentation)

Remote Desktop Connection

This selection opens the Remote Desktop Connection dialog box. This dialog box, which also opens from a desktop icon, is used to establish connections to remote applications using RDP. Refer to the Microsoft Web site for documentation that offers a detailed explanation and instructions on how to use the Remote Desktop Connection dialog box.

TeemNT

The TeemNT terminal emulation application is installed on the terminal. Refer to the terminal emulation documentation (supplied separately) for complete instructions. By default, a desktop icon is not installed.

Internet Explorer

Version 6.0 of the Microsoft Internet Explorer browser is installed locally on the thin client.

The Internet options settings for the browser have been preselected at the factory to limit writing to the flash memory. These settings prevent exhaustion of the limited amount of flash memory available and should not be modified. The user may access another browser through an ICA or RDP account if more browser resources are required. The local browser opens from the Start menu or from a desktop icon.

Control Panel Extended Selections

The Control Panel window is accessed by clicking **Start** on the task bar and selecting **Start > Control Panel.** Some of the extended selections available on the Control Panel are discussed in the following sections.

HP RAMDisk

The RAM disk is volatile memory space set aside for temporary data storage. It is the Z: drive shown in the My Computer window.

The following items are stored on the RAM disk:

- Browser Web page cache
- Browser history
- Browser cookies
- Browser cache
- Temporary Internet files
- Print spooling
- User/system temporary files

The RAM disk may also be used for temporary storage of other data (such as roaming profiles) at the administrator's discretion (see "Local Drives" on page 34 of this guide).

Use the Ramdisk Configuration dialog box to configure the RAM disk size. If you change the size of the RAM disk, you will be prompted to restart for changes to take effect, but to permanently save the change be sure that the write filter cache has been disabled or that the **-commit** command has been issued during the current boot session before restarting.

The default RAM disk size may vary depending on the thin client model and the installed memory size. The maximum Ramdisk size that can be set is 64 MB, the minimum is 2 MB.

Regional and Language Options

The keyboard language options are preset at the factory. Should you need to make a change, the keyboard language selection is made through the **Regional and Language Options** selection in the Control Panel. From this program you can select the type of keyboard you are using as well as the layout/IME settings.

An IEPC keyboard is required for any language other than English (US). The keyboard layouts are different for each of the languages listed above.

Administrative Tools

Click on the Administrative Tools icon in the Control Panel to open a window containing the administrative tool selections.

Services

The Services selection opens the Services window, which lists the services installed on the thin client.

User Manager

User Manager is the utility that allows the administrator to create, delete, and maintain user accounts. For more information see “User Profiles” on page 37 of this guide.

Peripherals

Depending on the ports available on the thin client, the thin client can provide services for USB, serial, parallel, and PCI devices, as long as the appropriate software is installed. Factory-installed software is described in the following section. Add-ons for other services, as they become available, can be installed using the Altiris Deployment Solution software (discussed in “Firmware Upgrades” on page 39).

USB to Serial Converter Cable

Use this procedure to determine the port assigned to a device connecting to the thin client through a USB to serial converter cable.

1. Connect a printer or other device to the serial port of the converter cable. Do not connect the USB end of the converter cable to the thin client at this time.
2. Open the Device Manager window (**Control Panel > System > Hardware Tab > Device Manager**).
3. A Ports (COM & LPT) listing may or may not be present, depending on the thin client model and whether a device driver was previously installed to a port. If the listing is present, expand it so that ports presently used are displayed.
4. Plug in the USB end of the converter cable to the thin client.

5. The Ports (COM & LPT) listing will appear if not already present. Under the Ports (COM & LPT) listing, a new COM port will appear for the new connection. Note which COM port number is assigned to the new connection.
6. Continue the installation procedure for the connected device, using the discovered port number when prompted. Use the manufacturer's procedures for other devices such as a serial touch screen.

No more than two USB to serial converters may be used at one time.

Printers

A universal print driver is installed on the thin client to support text-only printing to a locally connected printer. To print full text and graphics to a locally connected printer, install the driver provided by the manufacturer and follow the manufacturer's instructions. Be sure to disable the write filter cache or run the **-commit** command to save the installation. Printing to network printers from ICA and RDP applications can be achieved through print drivers on the servers.

CAUTION: If the available free space on the flash memory is reduced to below 3 MB, the thin client becomes unstable.

For printers to work and be downloaded, there must be sufficient flash space available. In some cases it may be necessary to remove software components to free up space for printers.

Printing to a locally-connected printer from an ICA or RDP session using the print drivers of the server produces full text and graphics functionality from the printer. To do this, you must have the print driver installed on the server and the text-only driver installed on the thin client (see the following section).

Adding Printers—Using Generic Text Only Print Driver

Follow these steps to add a printer using the text-only print driver:

1. Connect the printer to the parallel port.
2. Choose Printers and Faxes from the **Start > Settings** menu.
3. Double-click on **Add a Printer.** This opens the Add Printer Wizard.
4. Click **Next** in the first panel of the wizard.
5. Select the Local printer configured to this computer radio button.
6. Verify that the Automatically Detect and Install my Plug and Play Printer check box is **not** selected.
7. Click **Next.**
8. Select the Use the Following Port: radio button.
9. Select the appropriate port from the drop-down list and click **Next.**
10. Choose the Manufacturer and Model of the printer and click **Next.**
11. Use the assigned default name or other name for the printer and click **Next.**
12. Select the Do Not Share this Printer radio button and click **Next.**
13. Choose whether to print a test page or not and then click **Next.**
14. Click **Finish.**
15. The installation will complete and a test page will print if this option was chosen.

Using the Manufacturer's Print Drivers

Install the driver provided by the manufacturer and follow the manufacturer's instructions. Be sure to disable the write filter or issue the **-commit** command to save the installation.

Audio

Audio may be redirected from applications to the audio jacks on the thin client. The level must be controlled externally (such as by a 600-ohm potentiometer control) and a power booster is required to drive speakers. The volume can be adjusted using the sound icon in

the task bar system tray. You can single-click on this icon to open the master volume control, or double-click to open the volume control application dialog box.

Microsoft Windows XPe Service Pack 2 (SP2)

Microsoft Windows XPe Service Pack 2 (SP2) addresses new challenges to the security of personal computers by making a number of basic improvements to the operating system.

The HP Compaq Thin Clients Microsft XPe SP2 Image includes improvements to the following features:

- Network Protection
- Microsoft Internet Explorer
- Windows Messenger
- Windows Media Player

Network Protection

Network protection is the largest area of improvement in Windows XPe Service Pack 2, and the one with the most implications for existing software.

Sygate Firewall

HP's XPe SP2 image includes a Sygate firewall. HP Sygate Security Agent provides a customizable firewall that helps protect your computer from intrusion and misuse, whether malicious or unintentional. It detects and identifies known Trojans, port scans, and other common attacks, and in response, selectively allows or blocks the use of various networking services, applications, ports, and components.

HP Sygate Standalone Agent has the ability to allow or block any port or protocol, inbound or outbound, by either application or traffic signature. The Agent not only blocks according to these parameters, but can also link them with logical and/or conditional statements, increasing the scope and flexibility of polices that can be applied. The Agent can also block and apply policy to custom protocol adapters, enabling enterprises to use custom network-enabled applications and to block applications that circumvent the TCP/IP stack with custom protocol adapters.

Additional information about the Sygate Firewall is available in the "HP Sygate Security Agent: Frequently Asked Questions" white paper:

http://h200006.www2.hp.com/bc/docs/support/SupportManual/c00282639/c00282639.pdf

Microsoft Windows Firewall

An improved Microsoft Windows Firewall (previously known as Internet Connection Firewall, or ICF) is available from HP as an add-on. The firewall is enabled by default once the add-on is installed.

The Microsoft Windows Firewall is provided only as an add-on, and is not included in the image. Before installing the Microsoft Windows Firewall, the Sygate Firewall must be removed. A Sygate Firewall removal add-on is available at http://h18004.www1.hp.com/support/files/thinclients/us/download/22239.html

On-By-Default

Once the add-on is installed, Windows Firewall will be turned on by default for all network interfaces. On-by-default also protects new network connections as they are added to the system. This might break application compatibility if the application does not work with stateful filtering by default.

Configuring Microsoft Windows Firewall

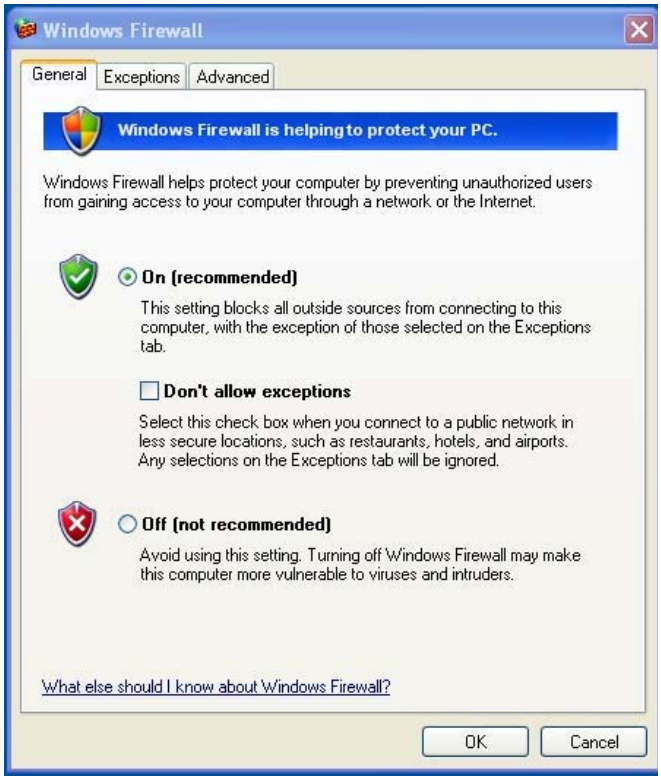
In order to provide the best security and usability, Windows Firewall provides the ability to add exceptions for applications and services so that they can receive inbound traffic.

To configure Windows Firewall, open the firewall itself from Control Panel. Another option for accessing the firewall configuration is on the Advanced tab in network connection properties.

Security Center is not in the image. Once the Windows Firewall Add-on is applied, the FIREWALL.CPL control panel applet will only be available for the Administrator account.

Once the Windows Firewall Add-on is launched, the control panel applet will only be available to the administrator account. .

- **General Tab**: The General tab provides access to the main three configuration options as shown below.
  - On (Recommended)
  - Don’t allow exceptions
  - Off (Not Recommended)



When you select Don't allow exceptions, Windows Firewall blocks all requests to connect to your computer, including those from programs or services on the Exceptions tab. The firewall also blocks file and printer sharing, and discovery of network devices.

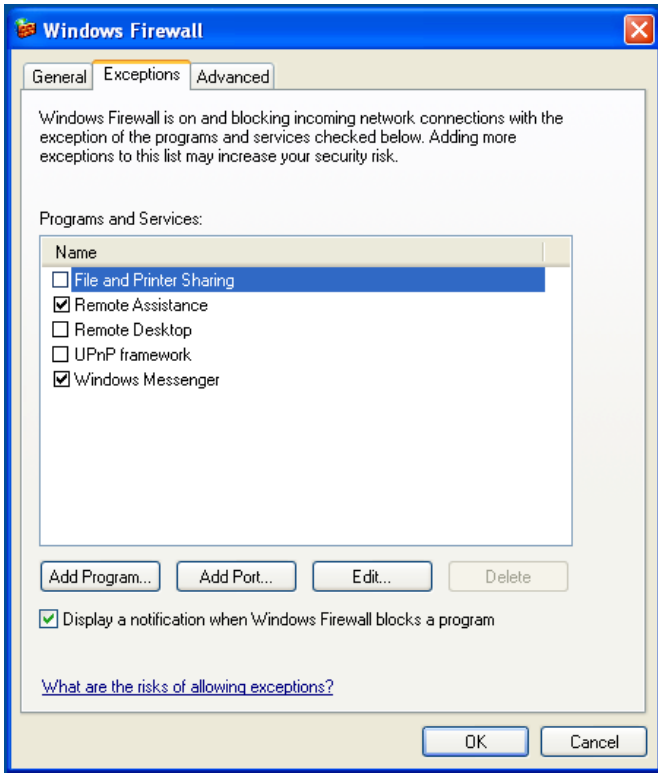
Using Windows Firewall with no exceptions is useful when connecting to a public network, such as one at an airport or hotel. This setting can help to protect your computer by blocking all attempts to connect to your computer.

When you use Windows Firewall with no exceptions, you can still view Web pages, send and receive e-mail, or use an instant messaging program.

- **Exceptions Tab**: Provides the ability to add Program and Port exceptions to permit certain types of inbound traffic. The exception settings specify the set of computers for which this port/program is open.

  You can specify three different modes of access:

  - Any computer (including those on the(Internet)
  - My network (subnet) only
  - Custom list

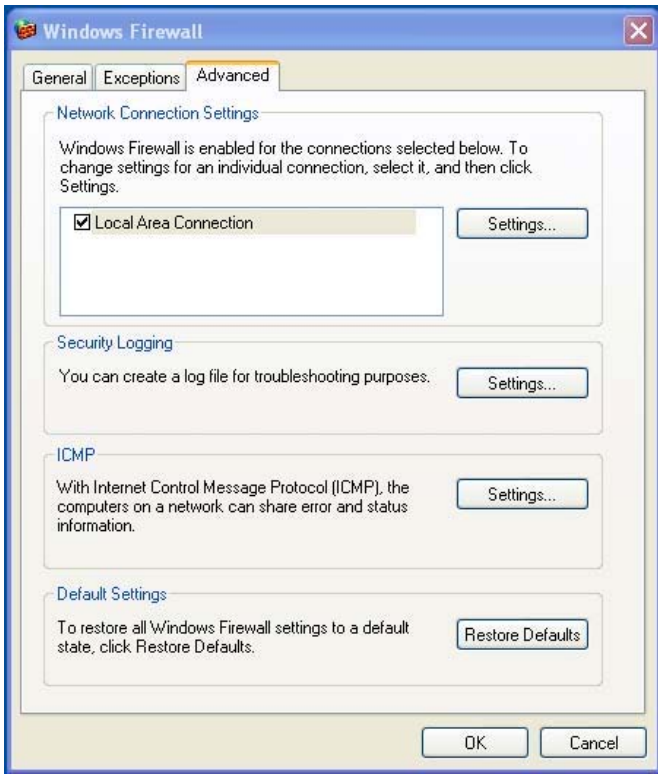


The checkbox "Display a notification when the Windows Firewall blocks a program" will be checked by default.

For each exception, you can set a scope for the exception. For home and small office networks, it is recommended that you set the scope to the local network only where possible. This will

enable computers on the same subnet to connect to the program on the machine, but drops traffic originating from a remote network

- **Advanced Tab:** Enables you to configure the following functions.
  - **Network Connection Settings:** Select connection-specific rules which apply per network interface.
  - **Security Logging:** Create a log file for troubleshooting.
  - **ICMP:** With Global Internet Control Message Protocol (ICMP) the computers on a network can share error and status information.
  - **Default Settings:** Restore Windows Firewall to a default configuration.



Gathering Configuration Information

To examine the current policy configuration for Windows Firewall you can use the following command: **netsh firewall show configuration**.

Troubleshooting Applications

Modifying an application to work with a stateful filtering firewall is the ideal way to resolve issues. This is not always possible, so the firewall provides an interface for configuring exceptions for ports and applications.

Failure Symptoms

Failures related to the default configuration will manifest in two ways:

- Client applications may fail to receive data from a server. Examples would be an FTP client, multimedia streaming software, and new mail notifications in some email applications.
- Server applications running on the Windows XP computer may not respond to client requests. Examples would be a Web server such as Internet Information Services (IIS), Remote Desktop, and File Sharing.

Failures in network applications are not limited to firewall issues. Failures could be caused by RPC or DCOM security changes. It is important to note whether the failure is accompanied by a Windows Firewall Security Alert indicating that an application is being blocked.

Resolution

With either of the failures mentioned above, you can add exceptions to the configuration for Windows Firewall. Exceptions configure the firewall to permit specific inbound connections to the computer.

HP recommends adding a program rather than adding a port. Adding a program is easier and safer than adding a port: it is not necessary to know which port numbers to use and because the port is only open when the program is waiting to receive a connection. Only the specified application can use the port, whereas opening a port allows any applicationto use it.

Adding a Program

The recommended configuration to try is adding a program to the exception list. This provides the easiest configuration, as well as enabling the firewall to open ranges of ports that could change each time the program runs.

The steps to add a program exception are:

1. Open Windows Firewall and click the Exceptions tab.
2. If the program is in the list, click to enable the setting. If the program is not in the list, click Add Program to display the Add a Program dialog box.
3. Click Browse to choose the program you wish to add as an exception, and then click OK.

4. Click Change Scope to view or set the scope for the program and then click OK.
5. Click OK to close the Add a Program dialog box.
6. By default, the program is not enabled in the list. Click the check box to enable the program.

Adding a Port

If adding the program to the exception list does not resolve the application issue, you can add ports manually. To do this you will first need to identify the ports used by the application. The most reliable method for determining the port usage is to consult with the application vendor.

If the port number(s) for the process are less than 1024, it is likely that the port numbers will not change. If the numbers used are greater than 1024, the application may be using a range of ports, so opening individual ports may not resolve the issue reliably.

Once you have the port number and protocol, add an exception for that port. To add a port exception, perform the following steps:

1. Open Windows Firewall and click the Exceptions tab.
2. Click Add Port to display the Add a Port dialog box.
   a. Enter the Port Number.
   b. Choose TCP or UDP protocol.
   c. Give the port exception a descriptive name in the Name field.
3. Click Change Scope to view or set the scope for the port exception, click OK.
4. Click OK to close the Add a Port dialog box.
5. Click to enable the port.

Additional Resources

Refer to the following resources for additional Microsoft Windows Service Pack 2 and Microsoft Windows Firewall information:

- Windows XP Service Pack 2: A Developer's View
  http://msdn.microsoft.com/security/default.aspx?pull=/library/en- us/dnwxp/html/securityinxpsp2.asp
- TechNet Windows XP Professional Web site
  http://www.microsoft.com/technet/prodtechnol/winxppro/default.mspx
- Manually Configuring Windows Firewall in Windows XP Service Pack 2
  http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx
- Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2
  http://www.microsoft.com/downloads/details.aspx?FamilyID=cb307a1d-2f97-4e63-a581- bf25685b4c43&displaylang=en
- Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2
  http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1&displaylang=en

Microsoft Internet Explorer

Microsoft Internet Explorer has been made much more secure in Service Pack 2. It has more control over the execution of all content. Internet Explorer now has a built-in facility to block unwanted pop-up windows, and manage the viewing of desired pop-up windows. Furthermore, Internet Explorer now keeps scripts from moving or resizing windows and status bars to hide them from view or obscure other windows.

Windows Messenger

A block unsafe file transfers feature has been added to Windows Messenger in Windows XPE Service Pack 2.

For a list of files that are generally considered unsafe, see "Information About the Unsafe File List in Internet Explorer 6" on the Microsoft Web site at http://go.microsoft.com/fwlink/?LinkId=25999

Windows Media Player 9

The new Media Player contains security, performance, and functionality improvements.

For more information about improvements to Windows Media Player, refer to the Windows Media Player home page at http://www.microsoft.com/windows/windowsmedia/

Utilities and Settings

This section describes some of the utilities and settings found on your thin client.

Enhanced Write Filter Manager

The Enhanced Write Filter Manager provides a secure environment for thin-client computing. It does this by protecting the thin client from undesired flash memory writes (flash memory is where the operating system and functional software components reside). The write filter also extends the life of the thin client by preventing excessive flash write activity. It gives the appearance of read-write access to the flash by employing a cache to intercept all flash writes and returning success to the process that requested the I/O.

The intercepted flash writes stored in cache are available as long as the thin client remains active, but will be lost when the thin client is rebooted or shut down. To preserve the results of writes to the registry, favorites, cookies, and so forth, the contents of the cache can be transferred to the flash on demand by the Altiris Deployment Solution software or manually using the Enhanced Write Filter Manager.

After the write filter has been disabled, all future writes during the current boot session are written to the flash, with no further caching until a reboot occurs. The write filter may also be enabled/disabled through the command line. Always enable the writer filter after all of your permanent changes have been successfully made.

The administrator should periodically check the status of the cache. The thin client should be rebooted if the cache is more than eighty percent full.

CAUTION: The write filter cache should never be disabled if it is 80 percent or more full.

To avoid flash corruption when administering the thin client for permanent changes, it is strongly recommended the write filter cache be disabled before making permanent modifications to the system. Remember to enable writer filter after all your changes have been made.

The following section describes how the write filter can be manipulated through the command line.

Enhanced Write Filter Manager Command Line Control

CAUTION: Terminal Administrators should use Microsoft Windows NT file security to prevent undesired usage of these commands.

CAUTION: When using the **-commit** command, all the temporary contents are permanently written to the flash memory.

Because the Enhanced Write Filter Manager commands are executed on the next boot, you must reboot the system for the command to take effect.

Windows XPe includes the Enhanced Write Filter (EWF) console application command line tool, Ewfmgr.exe, and can be used to issue a set of commands to the EWF driver, report the status of each protected volume overlay, and report the format of the overall EWF configurations.

By including the EWF Manager console application component in your configuration and building it into your image, you enable use of Ewfmgr.exe and the corresponding commands.

To use the Enhanced Write Filter Manager using the command line, select **Start > Run > Open** and access the system DOS prompt by typing **CMD** in the Open field and clicking **OK.**

At the system prompt enter **ewfmgr c:** and press **Enter.** Using the **ewfmgr <drive-letter> -[boot command]** syntax, use the following commands in the **boot command** variable of the command line:

-all

Displays information about all protected volumes and performs a command, such as disable, enable, and commit, on each volume, if specified.

-commit

This command commits all current level data in the overlay to the protected volume, and resets the current overlay value to 1. -commit can be combined with the -disable command to commit and then disable.

-disable

This command disables the overlay on the specified protected volume.

-enable

This command enables the Enhanced Write Filter so that data written to the protected media is cached in the overlays. The current overlay level becomes 1 as soon as EWF is started, and a new overlay is created at level 1.

-commitanddisable

Combination of the “Commit” and “Disable” commands. This command will commit data in the overlay upon shutdown. Additionally, EWF will be disabled after the system reboots.

Enhanced Write Filter GUI

In addition to the DOS command-line tool, the Windows XP Embedded image now includes an Enhanced Write Filter (EWF) GUI. The EWF GUI can be accessed through the Control Panel or the Administrative Tools option for the administrator. To access the EWF GUI, perform the following steps:

1. Log in as an administrator
2. Select **Start > Control Panel > Other Control Panel Options** or S**tart > Control Panel > Performance and Maintenance > Administrative Tools.**

3. Click the **EWF Manager** icon.
4. Use the EWF GUI to Select Write Filter options.

The EWF GUI includes the following buttons:

Enable EWF

This button is the same as executing **ewfmgr.exe c: -Enable** from the DOS prompt.

Disable EWF

This button is the same as executing **ewfmgr.exe c: -Disable** from the DOS prompt.

Overlay Configuration

This button simply displays the Overlay information and is a combination of the information supplied when executing **ewfmgr.exe c: -Description** and **ewfmgr.exe c: -Gauge** from the DOS prompt.

Clear Boot Command

This button is the same as executing **ewfmgr.exe c: -NoCmd** from the DOS prompt.

Commit Data to Volume

This button is the same as executing **ewfmgr.exe c: -Commit** from the DOS prompt.

Enhanced Write Filter Status Tool

Windows XPe Image Refresh 5.1.033 includes the EWF status service. This service creates an icon in the System Tray that shows the status of EWF. The EWF Status icon will appear as a red "lock" when disabled, a green "lock" when enabled, and a yellow "lock" when the state is set to change on next boot.

In the event of a corrupted EWF state, you will need to re-flash the thin client unit with the standard shipping image provided on the web. For additional information, please see the "HP Compaq Thin Client Imaging Tool" white paper located at: http://h200006.www2.hp.com/bc/docs/support/UCR/SupportManual/TPM_339082-003_rev4_us/TPM_339082-003_rev4_us.pdf.

If you are logged-on as Administrator, you can change the status of EWF by right-clicking on the icon and select the desired EWF state.

Since EWF Manager console utility (ewfmgr.exe) and the EWF status service execute separate code, any status changes by ewfmgr.exe will not be automatically reflected by the EWF status icon.

If you modify the EWF through the command line, you must right-click on the icon (you can then click anywhere on the screen to close the context menu) to refresh the status icon display. The status icon display is refreshed automatically when you make modifications through the EWF Control Panel applet. The EWF applet always reflects the current status.

Local Drives

The following sections describe the local drives located on the thin client.

Drive Z:

Drive Z: is the onboard volatile memory (Ms-ramdrive) on the logic board of the thin client. Because drive Z: is volatile memory, it is recommended that you do not use this drive to save data that you want to retain. See “HP RAMDisk” on page 13 for Ramdisk

configuration instructions. Also see “Roaming Profiles” on page 36 of this guide for information about using the Z: drive for roaming profiles.

Drive C: and Flash

Drive C: is in the onboard non-volatile flash memory. It is recommended that you do not write to drive C:. Writing to drive C: reduces the free space on the flash.

CAUTION: If the available free space on the flash memory is reduced to below 3 MB, the thin client becomes unstable.

The Enhanced Write Filter (if enabled) protects the flash from damage and presents an error message if the cache is overwritten.

Items that are written to the write filter cache (or directly to the flash, if the write filter has been disabled) during normal operation include Favorites, created connections, and deleted or edited connections.

Saving Files

CAUTION: The thin client uses an embedded operating system with a fixed amount of flash memory. It is recommended that you save files that you want to retain on a server rather than on your thin client. Be careful of application settings that write to the C: drive, which resides in flash memory (in particular, many applications by default write cache files to the C: drive on the local system). If you **must** write to a local drive, change the application settings to use the Z: drive. To minimize writing to the C: drive, the configuration settings should be made as described in the “User Log Accounts” section that follows.

Mapping Network Drives

You can map network drives if you log on as either Administrator or User. To keep the mappings after the thin client is rebooted you must:

1. Disable the write filter cache during the current boot session or issue the **-commit command.**
2. Select the Reconnect at Logon check box.

Because a user logon cannot disable the write filter cache, the mappings can be retained by logging off the user (do not shut down or restart) and logging back on as Administrator, and then disabling the write filter.

A remote home directory also may be assigned by using a user manager utility or by other means known to administrators.

Roaming Profiles

Write roaming profiles to the C: drive. The profiles need to be limited in size and will not be retained when the thin client is rebooted.

For roaming profiles to work and be downloaded, there must be sufficient flash space available. In some cases it may be necessary to remove software components to free up space for roaming profiles.

User Log Accounts

This section describes how to create a new user account and user profile.

Creating a New User Account

CAUTION: Be sure to disable the write filter cache during the boot session in which a new account is created. Remember to enable the write filter after all of your permanent changes have been saved to flash.

You must be logged on as administrator to create user accounts, which you can do locally or remotely. Due to local flash/disk space constraints, the number of additional users should be kept to a minimum.

New user accounts are created with the User Manager utility. To access this utility, click **Control Panel > Performance and Maintenance > Administrative Tools.**

User Profiles

A new user profile will be automatically configured from a template based on the default user or administrator access settings in the registry, browser profiles, and ICA and RDP initial settings. If the default user or administrator profile settings are changed from those set at the factory, the changed settings are automatically applied to the new user profile.

For the new user to match the characteristics of the default user, the administrator must create the user in the user group and also add the new user to the administrator group. The default user is in both groups; otherwise the new user will not be able to add a local printer. The user's actions are still limited while the user is in the administrator group.

To create the user:

CAUTION: Because of the limited size of the flash memory, it is strongly recommended that other applications available to the new and existing users be configured to prevent writing to the local file system. For the same reason, it is also recommended that extreme care be exercised when changing configuration settings of the factory-installed applications.

1. Log in as administrator.
2. Open the Administrative Tools window (**Start > Control Panel > Performance and Maintenance > Administrative Tools**).
3. Double-click **User Manager** to open the Local Users and Groups window.
4. Double-click the Users folder to view the contents in the right pane.
5. Click **Action** in the menu bar and select New User in the drop-down menu. This opens the New User dialog box.
6. Type in the user name and password, and select the attributes you want.
7. Click **Create,** then click the **Close** command button.

8. In the Local Users and Groups window, select (highlight) the Users folder in the left pane.
9. In the right pane, double-click the name of the user just created. This opens the [user name] Properties tabbed dialog box.
10. Open the **Member Of** tab dialog.
11. Click **Add.** This opens the Select Groups dialog box.
12. Type **Administrators** in the field labeled Enter the Object Names to Select. This will enable the Check Names command button.
13. Click **Check Names,** then click **OK.**
14. The newly created user will now be a member of both the administrators and users groups and should match the privileges of the default user account.

Remote Administration and Firmware Upgrades

This section will highlight and discuss the Remote Administration capabilities and firmware upgrade methods applicable to your thin client.

Altiris Deployment Solution Software

The Altiris Deployment Solution software is a full-featured remote administration tool set. It accesses the thin client through the Altiris remote Agent and PXE server utilities installed on the thin client. Altiris allows the thin client administration functions (including firmware upgrades) to be performed without requiring an administrator to visit the individual thin client sites.

For specific information on using Altiris, consult the Altiris help documentation.

Add-on Modules

If it is desired to install an add-on module, the administrator must use the Altiris Deployment Solution for administering the thin client. The write filter should be disabled/enabled as needed to save the changes.

CAUTION: If the available free space on the flash memory is reduced to below 3 MB, the thin client becomes unstable.

For add-on modules to work and be downloaded, there must be sufficient flash space available. In some cases it may be necessary to remove software components to free up space for add-on modules.

Firmware Upgrades

The Intel Preboot Execution Environment (PXE) is a protocol that defines interaction between TCP/IP, DHCP and TFTP to enable a client to download a preboot environment from a server. PXE allows a client to boot from a server on a network prior to booting the embedded operating system or the operating system from the local flash module. PXE allows a network administrator to remotely wake up a thin client and perform various management tasks, including loading the operating system and other software onto the thin client from a server over the network. The PXE client is installed on the thin client and the PXE server component is part of the Altiris Deployment Solution suite.

Citrix ICA auto update does not function for the ICA client installed on the thin client; updates are implemented through the standard firmware upgrade process.

HP Compaq Thin Client Imaging Tool

The HP Compaq Thin Client Imaging Tool is part of the Softpaq deliverable that contains the original factory image for the HP Compaq t5000 thin client. This utility can be used to restore the original factory image to your thin client.

With this utility you have three options. You can:

- Generate and ISO image to use with CD creation software to create a bootable CD for deployment using a USB CD-ROM drive.
- Create a bootable flash image on a USB flash device (such as on a disk on key).
- Unbundle the image to a directory for use in a custom deployment scenario or PXE image.

For additional information about this utility and its uses, visit the HP Web site at

http://www.hp.com/products/thinclientsoftware